Una nueva ciberseguridad frente a amenazas desconocidas

KASPERSKY lab

La nueva ciberseguridad frente a amenazas desconocidas

La ciberseguridad está cambiando, al igual que la tecnología, las empresas, el mercado, el uso de los datos y, sobre todo, las intenciones de los cibercriminales. Ya no se trata de llamar la atención, sino de todo lo contrario, de buscar una brecha por la que colarse en la empresa y mantenerse ahí, robando ingentes cantidades de datos, de la forma más sigilosa y continuada posible.

La realidad es que, de las brechas de malware, el 70 por ciento son amenazas conocidas, el 29 por ciento son desconocidas y solo el 1 por ciento son de las denominadas amenazas avanzadas. Defenderse contra amenazas conocidas es relativamente sencillo: en el momento en que se reconoce el código, se bloquea, algo que hacen sin problemas con métodos tradicionales como los basados en firmas. En cambio, luchar contra ese 29 por ciento de amenazas desconocidas es más complejo y requiere herramientas más sofisticadas, si bien, empleando herramientas que amplíen las posibilidades de los tradicionales antivirus, como la heurística o las listas blancas dinámicas, se pueden combatir también.

Pero, ¿qué pasa con el 1% restante? Las amenazas avanzadas tienen diferentes apariencias, son continuas y representan ataques dirigidos. Están diseñadas para penetrar en la red, permanecer ocultas y recolectar datos sensibles, con el objetivo de no ser detectadas durante el mayor tiempo posible. Con la operativa típica de las APT(Advanced Persistent Threats), que operan en silencio y durante mucho tiempo, los daños pueden ser muy importantes, tanto por los datos robados como por las caídas del sistema e, incluso, por los

La realidad es que, de las brechas de malware, el 70 por ciento son amenazas conocidas, el 29 por ciento son desconocidas solo el 1 por ciento son de las denominadas amenazas avanzadas

efectos reputacionales. Por este motivo, la prevención es, de lejos, una opción menos costosa que cualquier remedio que se quiera usar una vez descubierta, dado que esto puede suceder meses o, incluso, años, después de haber ocurrido.

Empresas: objetivos de alto interés

El primer paso para crear una estrategia adecuada frente a estas amenazas es comprender que su empresa es un objetivo potencial. Incluso aunque pueda pensar que los datos que maneja no son interesantes para los atacantes, aunque seguro que sí lo son, pueden aprovechar su infraestructura para llevar sus ataques a clientes o proveedores, como ocurrió con el caso del denominado Darkhotel.

Es necesario, en segundo lugar, detectar los posibles puntos de entrada, algo más crítico cuanto más grande y distribuida sea una empresa. En este sentido, el BYOD y las herramientas de trabajo flexible no hacen sino incrementar el reto.

En un entorno como el actual, la diversidad y amplitud de los endpoints, junto con la diversidad de métodos de ataque, hace que las medidas simples no sean suficientes. Frente a esto, son necesarias unas medidas robustas que aúnen inteligencia, políticas de seguridad y tecnología especializada, no solo para hacer frente a las amenazas conocidas actualmente, sino también a las nuevas que surjan.

Por último, la mitigación debe incrementar el foco sobre los puntos de acceso. De hecho, si estos puntos de acceso no cuentan con una adecuada protección multicapa, toda la organización estará en riesgo.

¿Cómo mitigar los efectos de estas amenazas?

Dice el refrán, "más vale prevenir…" Pues bien, esto es totalmente cierto en el caso de las APT, donde arreglar los efectos es mucho menos efectivo en coste que prevenir las amenazas. Pero, ¿cómo hacerlo? ¿Qué debe incluir una estrategia adecuada? En primer lugar, políticas de seguridad y formación adecuada, porque la seguridad IT no depende solo de la tecnología. En segundo lugar, debemos aplicar una estructura de red que permita mitigar las amenazas, como es el caso, por ejemplo, de la segregación de ciertas secciones que pueden mitigar los riesgos. Tercero, administrando correctamente las políticas y privilegios de uso de los usuarios, se puede reducir de forma considerable el número de amenazas. Por último, pero no por ello menos importante, contar con soluciones especializadas que puedan añadir nuevas capas de seguridad, como control de aplicaciones, parcheado de vulnerabilidades en estas aplicaciones o, incluso, en el sistema operativo. Otras posibilidades son la prevención de intrusiones basadas en host (HIPS), que restringe la actividad de las aplicaciones en función de su nivel de fiabilidad; o el análisis dinámico del correo electrónico y del contenido web.

Con todo, la clave está en aportar inteligencia para identificar y detener las amenazas y contar con los servicios adecuados en caso de que se produzca un ataque, servicios tales como análisis del malware, servicios forenses digitales o servicios de respuesta a incidentes.

Alfonso Ramírez, director general de Kaspersky Lab Iberia:

"Somos ciberseguridad, innovación y tecnología"

Las nuevas amenazas imponen un nuevo estilo en la ciberseguridad, lo que ha llevado a Kaspersky Lab a reorientar su estrategia de negocio, que les ha permitido salir de la tradicional protección del endpoint hacia una visión más global de la protección de las empresas. Su director general en España y Portugal nos ofrece más detalles.

¿Cuáles son las principales tendencias actuales en el mundo de la seguridad?

El cibercrimen no descansa y ya asoman nuevas amenazas a las que hacer frente. Este año veremos cómo el espionaje se pasa a los dispositivos móviles; se pondrán de moda los implantes pasivos, que casi no muestran señales de infección en el sistema; y aumentará la popularidad de las infecciones cortas.

Muchas infraestructuras críticas están conectadas a Internet y no siempre con la protección necesaria, con el peligro que esto supone. Asimismo, pronosticamos un aumento del ransomware, del cibersabotaje y del ciberespionaje dirigido a móviles e IoT. También crecerá la "mercantilización" de los ciberataques financieros con recursos especializados.

¿Cuáles son las principales amenazas a las que se enfrentan las empresas?

La evolución de las APT, el ransomware y amenazas financieras de alto nivel son los protagonistas de los

principales problemas de ciberseguridad este año en cuanto a amenazas corporativas se refiere. Según un análisis de Kaspersky Lab, basado en la inteligencia de Kaspersky Security Network, los ataques de ransomware contra empresas van en aumento, multiplicando por seis el número de ataques (de 27.000 en 2014-2015 a 158.600 en 2015-2016). En cuanto a las pymes en concreto, según el informe IT Security Risks 2016, más del 42% ha sido víctima del ransomware en los últimos doce meses. Una de cada tres compañías infectadas ha pagado el rescate y cerca del 18% no ha podido recuperar sus archivos, a pesar de hacer efectivo el pago reclamado. Además, no debemos olvidar que las PYME pueden ser una puerta de entrada a otras empresas.

¿Cómo debe ser la estrategia de seguridad de una empresa en este momento? ¿Qué aspectos debe tener en cuenta? ¿Qué elementos deben estar integrados en esta estrategia?

Además de llevar a cabo una seguridad reactiva ante incidentes, también es necesario que las empresas sean proactivas a la hora de plantear una estrategia de seguridad eficaz contra las nuevas tendencias cibercriminales. Las compañías no deben olvidar que la seguridad no es un "estado", sino un proceso. Es necesario proteger todas las plataformas, dispositivos y concienciar a los empleados en materia de seguridad para obtener una seguridad corporativa total, pues cada capa adicional de protección reduce el riesgo de penetración en la red.

ALFONSO RAMÍREZ, DIRECTOR GENERAL DE KASPERSKY LAB IBERIA

CLICAR PARA VER EL VÍDEO

¿Es posible contar con una seguridad adecuada basada en el perímetro de la red de la empresa? ¿Cómo debe ser el planteamiento actual de la seguridad?

El enfoque tradicional de seguridad ya no es adecuado para hacer frente a las ciberamenazas. El endpoint y el perímetro deben protegerse, pero es necesario ir un paso más allá de la detección y posterior resolución. La predicción y el análisis son fundamentales y hay que incorporarlos a cualquier estrategia de seguridad. Un elemento esencial para minimizar los riesgos de la seguridad TI corporativa debe centrarse en la educación y concienciación sobre ciberseguridad de los trabajadores para evitar que se conviertan en un agujero de seguridad.

"Kaspersky Lab es mucho más que una empresa de seguridad endpoint. Nuestro catálogo es uno de los más potentes en el sector del software de seguridad"

Y, en este escenario, ¿qué aporta una firma como Kaspersky Lab?

Desgraciadamente, muchas compañías utilizan una estrategia reactiva cuando ya se ha producido el ataque, es decir, se infectan y lo solucionan, o implementan una estrategia de seguridad y se olvidan. Es importante que las empresas vean la seguridad como un proceso y no como algo estático. Observar y estar alerta es una norma casi obligatoria. De hecho, desde Kaspersky Lab vemos la seguridad basada en cuatro pilares: predecir, prevenir, detectar y responder, y ofrecemos soluciones y servicios capaces de cubrir esas 4 necesidades. El catálogo de Kaspersky Lab de productos y servicios cubre totalmente esos 4 objetivos, para que la protección corporativa sea total: todos los dispositivos, redes, trabajadores concienciados, prevención e inteligencia, siempre con un servicio personalizado y adaptado a cada una de las necesidades empresariales que presenta cada cliente

¿Cómo ha cambiado la propuesta tecnológica de Kaspersky Lab?

Las empresas necesitan una combinación de tecnología, inteligencia y experiencia, y han de ver la seguridad como un proceso, en continua evolución, no como un estado (o únicamente un producto). Por eso desde Kaspersky Lab hemos dado un paso adelante y añadido a nuestra oferta de soluciones de seguridad TI una serie de servicios imprescindibles para proteger totalmente la red corporativa. Kaspersky Lab es mucho más que una empresa de seguridad endpoint. Nuestro catálogo es uno de los más potentes en el sector del software de seguridad. Somos ciberseguridad, innovación, tecnología. Desde la detección hasta la resolución de incidentes, pasando por el análisis y la detección.

Kaspersky Anti Targeted Attack: detección de ataques dirigidos y amenazas avanzadas

Las amenazas persistentes avanzadas (APT), los ataques dirigidos y el malware sofisticado son solo algunas de las nuevas amenazas en constante evolución a las que la empresa debe hacer frente. Una adecuada estrategia de seguridad debe trabajar en diferentes líneas: previsión, prevención, detección, y respuesta, y Kaspersky Anti Targered Attack se incluye en la labor de detección.

Es necesario un nuevo enfoque integrado y más flexible basado en los pilares de la predicción, prevención, detección y respuesta.

- Predicción: La formación de los empleados para reconocer las tácticas utilizadas en los ataques aumenta el análisis predictivo, igual que la capacidad de aprender de los errores mediante un análisis forense de las brechas; las pruebas de penetración, por su parte, pueden ayudar a destapar puntos débiles.
- Prevención: El fortalecimiento de los sistemas y la interposición de tantos obstáculos en el camino de los atacantes como sea posible son tan solo dos componentes de un enfoque integral que incluye limitar la capacidad de los ataques de propagarse y reducir su impacto.
- Detección: Se calcula que un ataque empresarial medio pasa desapercibido durante más de 200 días; cuanto antes se descubra un incidente, tanto mejor. Las tecnologías de detección respaldadas por el mejor análisis de amenazas aumentan la detección: a medida que evoluciona el ritmo de las amenazas, la mejor estrategia de detección se basa a menudo en la capacidad de detectar comportamientos y secuencias de eventos que indican que se ha producido una brecha. Y precisamente aquí es donde se integraría Kaspersky Anti Targeted Attack.

- Respuesta: Para ser eficaces, esas capacidades deben funcionar juntas como un sistema con varios niveles. Basada en inteligencia, centrada en las amenazas, integrada, integral y estratégica: estas son las características principales de una completa arquitectura de seguridad empresarial adaptable.

Detectar las amenazas en la red

Kaspersky Anti Targeted Attack es una plataforma de detección que implementa una serie de sensores dentro de la infraestructura del cliente que analizan el tráfico de red, correo, web, y puntos de acceso. Esta información se añade a la obtenida a partir de KSN (Kaspersky Security Network) y el servicio de inteligencia del fabricante, lo que constituye, de facto, un sistema de detección multicapa.

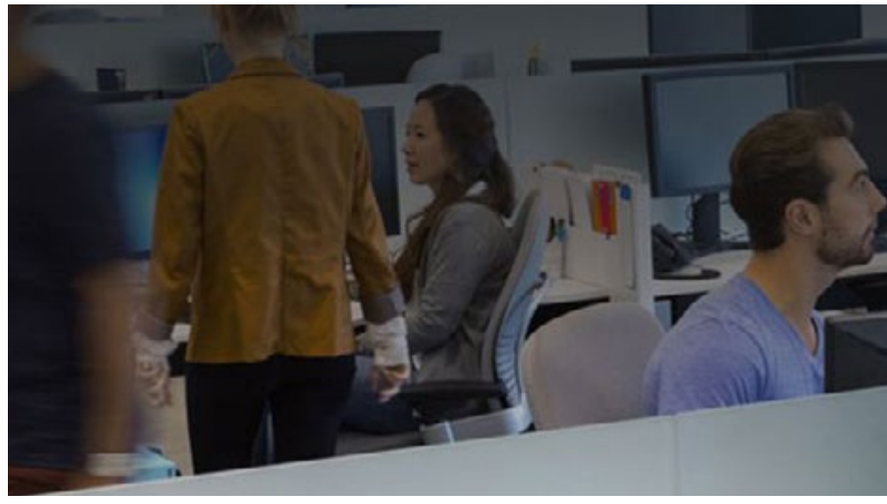
Alrededor de Kaspersky Anti Targeted Attack es posible agrupar algunos de los servicios ofrecidos por Kaspersky Lab, como, por ejemplo, Security Awareness Training, APT reports, Servicios Inteligencia, Servicios de consultoría, Incidence respond Service, entre otros.

Las empresas se enfrentan a problemas internos y externos a la hora de contar con una adecuada estrategia de seguridad. Empezando por los externos, encontramos las amenazas que aprovecha vulnerabilidades básicas, el factor humano, el cibercrimen como un servicio (CaaS) o los ataques a terceros, que pueden afectar a una empresa. Además, los internos, como la complejidad cada vez mayor de las TIC, el tiempo de detección de un ataque dirigido (214 días de media), seguridad dentro del perímetro, dado que el perímetro cada vez es más difuso.

Como decíamos en las primeras páginas, el porcentaje de amenazas de este tipo es muy pequeño, un 1%, pero las pérdidas que pueden generar son incalculables, de ahí que las empresas necesiten una respuesta, y ésta no puede darse si no tenemos una estrategia de seguridad basada en la inteligencia, y que vaya más allá de la prevención. De hecho, las empresas se gastan actualmente el 80-90% de su presupuesto en prevención y solo el resto en los otros aspectos, algo que podría cambiar en los próximos años, aunque el 60% previsto todavía no es suficiente.

Kaspersky Anti Targeted Attack detecta ataques dirigidos y amenazas sofisticadas que tradicionalmente un software de seguridad no puede identificar. Para ello, identifica objetos maliciosos basados en su comportamiento y en base a los datos obtenidos tanto de la experiencia como de otras fuentes de inteligencia.

A partir de ahí, entran en juego otras soluciones como Targeted Attack Analyzer, que detecta anomalías mediante el análisis de metadatos y relaciona la actividad con los datos recibidos por los sensores, o Sandbox, para aislar las posibles amenazas.



Kaspersky Anti Targeted Attack proporciona una detección avanzada que va más allá de la seguridad convencional centrada en la prevención

Servicios inteligentes:
la clave de la seguridad frente a las nuevas amenazas

Las empresas se exponen a diario a un gran número de ciberataques. Constantemente surgen amenazas sofisticadas y los cibercriminales están desarrollando técnicas innovadoras para superar las tecnologías de seguridad tradicionales. Las soluciones de seguridad tradicionales como los antivirus, el firewall y los sistemas de prevención de intrusiones no son suficientes para lograr una protección total. Es necesario recurrir a nuevas técnicas de protección para cubrir estas brechas de seguridad. Ése es el motivo por el que se ha desarrollado una gama de servicios basados en la inteligencia y experiencia de Kaspersky Lab.

Formación

La formación en ciberseguridad es fundamental para las empresas, que deben enfrentarse a cada vez más amenazas en constante evolución. El personal de seguridad debe formarse en el uso de técnicas de seguridad avanzadas porque es una pieza imprescindible de las estrategias de gestión y mitigación eficaces de las amenazas a la empresa.

¿Cómo puede consolidar y mejorar las destrezas de sus expertos en ciberseguridad? ¿Cómo reducir los riesgos de las consecuencias de un incidente? Kaspersky Lab ofrece una serie de programas de formación para varios niveles sobre análisis de malware y ciencia forense digital.

Concienciación en ciberseguridad

En torno al 80% de los ciberincidentes se deben a errores humanos. ¿Cómo puede mejorar los conocimientos en seguridad de sus empleados? Kaspersky Lab ofrece formación de concienciación en ciberseguridad con cursos presenciales y online.

Desde la compañía ayudan a los clientes a desarrollar una cultura de la ciberseguridad, gestionada por sus equipos de RR. HH. y de seguridad, con distintos pro-

Una nueva ciberseguridad frente a amenazas desconocidas

gramas de formación en concienciación, que utilizan la gamificación y están dirigidos a todos los niveles de la estructura de la organización.

Inteligencia frente a amenazas

¿Cómo puede mantenerse informado sobre las nuevas amenazas dirigidas a las empresas? ¿Qué ocurriría si su sistema SIEM no cuenta con la capacidad adecuada de detección de ciberamenazas? ¿Cómo puede recibir a tiempo notificaciones sobre las amenazas persistentes avanzadas más peligrosas? Kaspersky Lab ofrece una gama de servicios de inteligencia de amenazas diseñados para mitigar los siguientes riesgos:

- **Fuentes de datos de amenazas:** mejore la solución SIEM y la capacidad analítica con los datos sobre ciberamenazas de Kaspersky Lab.
- **Informes de inteligencia de APT:** disponga de acceso exclusivo y proactivo a descripciones de campañas de ciberespionaje de alto nivel y a indicadores de compromiso (IOC).
- **Informes de inteligencia de amenazas específicos para cada cliente:** una instantánea en el tiempo de la superficie de ataque que los cibercriminales han aprovechado, están aprovechando o aprovecharán para perpetrar el ataque a su organización. Se incluyen recursos críticos disponibles de manera pública e información confidencial filtrada, así como vectores de ataque de especial interés para desarrolladores de malware y cibercriminales.

Servicios expertos

¿Qué sucedería si su propia experiencia no fuera suficiente para resolver un ciberincidente? ¿Cómo puede asegurarse de que la infraestructura de IT o las aplicaciones están totalmente protegidas contra posibles ciberataques? Kaspersky Lab ofrece una gama de servicios expertos diseñados para mitigar y solucionar los siguientes riesgos:

- **Pruebas de introducción:** identifique los puntos más vulnerables de su infraestructura; evite daños económicos, interrupciones de la actividad y que su reputación se vea afectada por los ciberataques; cumpla con los estándares gubernamentales, industriales y corporativos (por ejemplo, PCI DSS).
- **Evaluación de seguridad de aplicaciones:** detecte vulnerabilidades en aplicaciones de cualquier tipo, desde soluciones basadas en la nube de gran envergadura, sistemas ERP, aplicaciones de banca online y otras aplicaciones específicas de su empresa hasta aplicaciones móviles e integradas para diferentes plataformas (iOS, Android…).
- **Análisis de malware y ciencia forense digital:** elabore una imagen detallada de cualquier incidente mediante exhaustivos informes con medidas para su solución.

Enlaces relacionados

- Prepárese para los riesgos del futuro
- Advanced Persistent Threats
- Kaspersky Anti Targered Attack
- Seguridad empresarial adaptativa
- Servicios inteligentes: Formación
- Servicios Inteligentes: Servicios Amenazas Inteligentes
- Servicios Inteligentes: Servicios Expertos